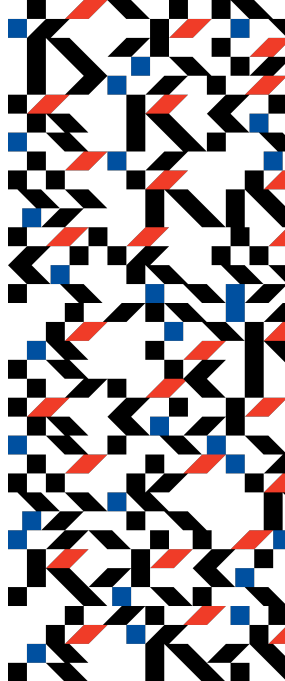


Неотслеживаемость по Шеннону для схем подписи вслепую

Утехина Мария Павловна
Ахметзянова Лилия Руслановна
Смышляев Станислав Витальевич

01.06.2026

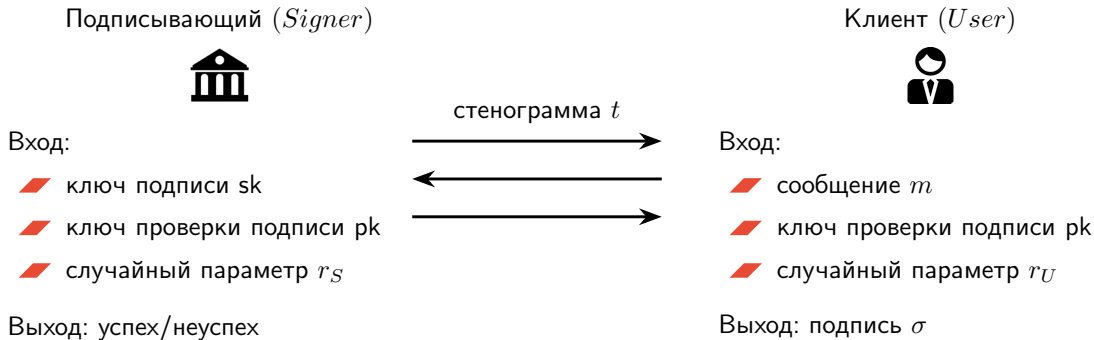


Подпись вслепую

- $(sk, pk) \leftarrow \text{KeyGen}(\)$: алгоритм генерации ключей;
- $(b, \sigma) \leftarrow \langle \text{Sign}(sk, pk), \text{User}(pk, m) \rangle$: интерактивный протокол, выполняемый между подписывающим, обладающим секретным ключом подписи sk и клиентом, обладающим сообщением m ;
- $b \leftarrow \text{Verify}(pk, m, \sigma)$: детерминированный алгоритм проверки подписи.

Протокол подписания

Рассматриваем двухраундовые схемы подписи вслепую с пустой первой пересылкой от клиента к подписывающему (схемы 2-BS).



Протокол подписания

Рассматриваем двухраундовые схемы подписи вслепую с пустой первой пересылкой от клиента к подписывающему (схемы 2-BS).

Подписывающий (*Signer*)



$$t^1 \leftarrow S_1(\text{sk}, \text{pk}, r_S)$$

Клиент (*User*)



$$t^1$$

$$t^2$$

$$t^3$$

$$t^2 \leftarrow U_1(\text{pk}, m, r_U, t^1)$$

$$t^3 \leftarrow S_2(\text{sk}, \text{pk}, r_S, t^2)$$

$$\sigma \leftarrow U_2(\text{pk}, m, r_U, t^1, t^3)$$

Неотслеживаемость

Неотслеживаемость (blindness): невозможность получения подписывающей стороной никакой информации о подписанном сообщении, где подписанное сообщение есть подпись сообщения, а также часть (возможно пустая) этого сообщения, не восстанавливаемая из подписи [1].

[1] - ГОСТ Р 34.14-2025 «Информационная технология. Криптографическая защита информации. Термины и определения.»



Модель BL (Juels A., Luby M., Ostrovsky R., 1997)

- Используется алгоритмический подход на основе экспериментатора (мера успешности нарушителя в модели характеризуется величиной $\text{Adv}_{2\text{-BS}}^{\text{BL}}(\mathcal{A})$).
- Основывается на задаче различения:
 - неочевидно соответствие с неформальным определением;
 - проблемы с нереалистичными условиями безопасной эксплуатации.

Результат

Наш результат:

- ▀ предложено новое определение неотслеживаемости — неотслеживаемость по Шеннону;
- ▀ доказана эквивалентность неотслеживаемости по Шеннону и совершенной стойкости в модели BL.

Неотслеживаемость по Шеннону

Необходимо задать:

- ▀ модель нарушителя;
- ▀ модель угроз.

Модель нарушителя

Нарушитель:

- ▀ выбирает открытый ключ pk ;
- ▀ взаимодействует с клиентом со стороны подписывающего.

Сообщение m выбирается клиентом.

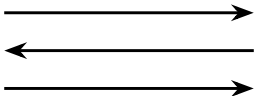
Нарушитель-подписывающий



Клиент ($User$)



стенограмма $t = (t^1, t^2, t^3)$



подпись σ

Нарушитель и клиент

▀ r_A, r_U, m выбираются в соответствии с распределением $\mathcal{D}_{r_A}, \mathcal{D}_{r_U}$ и $\mathcal{D}_m$.

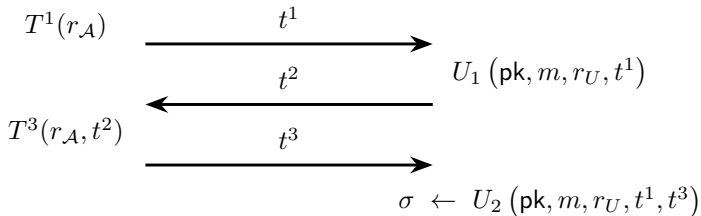
Нарушитель-подписывающий

$pk(r_A)$



Клиент (User)

$m \sim \mathcal{D}_m$



Модель угроз

Неотслеживаемость (blindness): невозможность получения подписывающей стороной никакой информации о подписанном сообщении, где подписанное сообщение есть подпись сообщения, а также часть (возможно пустая) этого сообщения, не восстанавливаемая из подписи [1].

Модель угроз. Получение нарушителем информации о подписанном сообщении.

Как формализовывать получение информации?

[1] - ГОСТ Р 34.14-2025 «Информационная технология. Криптографическая защита информации. Термины и определения.»



Неотслеживаемость по Шеннону

Как формализовывать получение информации?

Используем подход Шеннона для определения совершенных шифров.



Информация

Схема шифрования.

Шифр является совершенным, если для любого открытого текста его априорная и апостериорная (при условии наблюдения любого шифртекста) вероятности равны.



Информация по Шеннону

Схема шифрования.

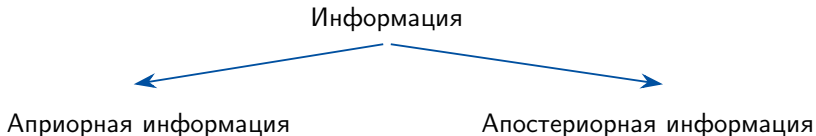
Шифр является совершенным, если для любого открытого текста его априорная и апостериорная (при условии наблюдения любого шифртекста) вероятности равны.



Схема подписи вслепую.

Гипотеза: схема 2-BS обладает неотслеживаемостью по Шеннону, если для любого подписанного сообщения его априорная и апостериорная (при условии наблюдения информации, передаваемой в рамках сеанса протокола) вероятности равны.

Априорная и апостериорная информация

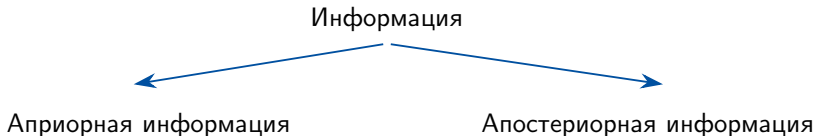


1. внешняя информация о сообщении:
 - распределение для m ;
2. описание алгоритма:
 - распределение для σ для любого m .

при условии наблюдения информации:

1. значения стенограммы t ;
2. информация о том, произошла на стороне клиента ошибка ($\sigma = \perp$) или нет ($\sigma \neq \perp$).

Априорная и апостериорная информация

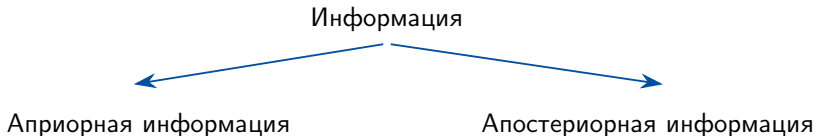


1. внешняя информация о сообщении:
 - распределение для m ;
2. описание алгоритма:
 - распределение для σ для любого m .

при условии **наблюдения** информации:

1. значения стенограммы t ;
2. информация о том, произошла на стороне клиента ошибка ($\sigma = \perp$) или нет ($\sigma \neq \perp$).

Априорная и апостериорная информация



1. внешняя информация о сообщении:
 - распределение для m ;
2. описание алгоритма:
 - распределение для σ для любого m .

при условии наблюдения и **влияния** на информацию:

1. значения стенограммы t ;
2. информация о том, произошла на стороне клиента ошибка ($\sigma = \perp$) или нет ($\sigma \neq \perp$).

Вероятностное пространство

Исходные условия.

- Распределения $\mathcal{D}_{r_A}$ на R_A , функция вероятности $p_{\mathcal{D}_{r_A}}(\cdot)$.
- Распределения $\mathcal{D}_{r_U}$ на R_U , функция вероятности $p_{\mathcal{D}_{r_U}}(\cdot)$.
- Распределения $\mathcal{D}_m$ на M , функция вероятности $p_{\mathcal{D}_m}(\cdot)$.

Вероятностное пространство:

- ▀ элементарный исход — (r_A, m, r_U) , $r_A \in R_A$, $m \in M$, $r_U \in R_U$;
- ▀ σ -алгебра — алгебра подмножеств множества элементарных исходов;
- ▀ вероятность события $A = \{(r_A^0, m^0, r_U^0), (r_A^1, m^1, r_U^1), \dots\}$ —

$$\Pr[A] = \sum_{(r_A^i, m^i, r_U^i) \in A} p_{\mathcal{D}_{r_A}}(r_A^i) \cdot p_{\mathcal{D}_m}(m^i) \cdot p_{\mathcal{D}_{r_U}}(r_U^i).$$



Случайные величины

Далее через $\{\tilde{\xi} = \xi\}$ будем обозначать событие, что случайная величина $\tilde{\xi}$ приняла значение ξ . В случае, когда необходимо подчеркнуть зависимость вероятности некоторого события от нарушителя $\mathcal{A}$, будем использовать обозначение $\Pr_{\mathcal{A}}[\tilde{\xi} = \xi]$.



Случайные величины

▀ Случайная величина, соответствующая значению сообщения:

$$\tilde{m}(r_A, m, r_U) = m.$$

▀ Случайная величина, соответствующая значению подписи:

$$\tilde{\sigma}(r_A, m, r_U) = U_2(pk(r_A), m, r_U, T^1(r_A), T^3(r_A, U_1(pk(r_A), m, r_U, T^1))) .$$

▀ Случайная величина, соответствующая значению стенограммы:

$$\tilde{t}(r_A, m, r_U) = (\tilde{t}^1(r_A, m, r_U), \tilde{t}^2(r_A, m, r_U), \tilde{t}^3(r_A, m, r_U));$$

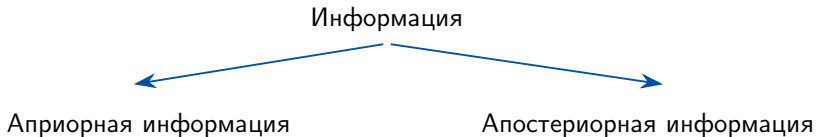
$$\tilde{t}^1(r_A, m, r_U) = T^1(r_A);$$

$$\tilde{t}^2(r_A, m, r_U) = U_1(pk(r_A), m, r_U, T^1);$$

$$\tilde{t}^3(r_A, m, r_U) = T^3(r_A, U_1(pk(r_A), m, r_U, T^1)) .$$



Априорная и апостериорная информация



1. внешняя информация о сообщении:

- $\Pr_{\mathcal{A}} [\tilde{m} = m];$

2. описание алгоритма:

- $\Pr_{\mathcal{A}} [\tilde{\sigma} = \sigma \mid \tilde{m} = m].$

при условии наблюдения и влияния на информацию:

1. значения стенограммы:

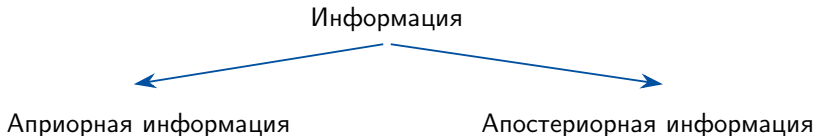
- $\Pr_{\mathcal{A}} [\dots \mid \tilde{t} = t];$

2. информация о том, произошла на стороне клиента ошибка или нет:

- $\Pr_{\mathcal{A}} [\dots \mid \tilde{\sigma} = \perp];$

- $\Pr_{\mathcal{A}} [\dots \mid \tilde{\sigma} \neq \perp].$

Априорная и апостериорная информация



1. внешняя информация о сообщении:

- $\Pr_{\mathcal{A}} [\tilde{m} = m];$

2. описание алгоритма:

- $\Pr_{\mathcal{A}} [\tilde{\sigma} = \sigma \mid \tilde{m} = m].$

при условии наблюдения и **влияния** на информацию:

1. значения стенограммы:

- $\Pr_{\mathcal{A}} [\dots \mid \tilde{t} = t];$

2. информация о том, произошла на стороне клиента ошибка или нет:

- $\Pr_{\mathcal{A}} [\dots \mid \tilde{\sigma} = \perp];$

- $\Pr_{\mathcal{A}} [\dots \mid \tilde{\sigma} \neq \perp].$

Неотслеживаемость по Шеннону

Определение

Схема 2-BS обладает неотслеживаемостью по Шеннону, если

- ▀ для любой стенограммы t ,
- ▀ для любого распределения $\mathcal{D}_m$, сообщения $m \in M$ и значения подписи $\sigma \neq \perp$,
- ▀ для любого нарушителя $\mathcal{A}$,

верно, что:

- если $\Pr_{\mathcal{A}} [\tilde{\sigma} \neq \perp, \tilde{t} = t] > 0$, то

$$\Pr_{\mathcal{A}} [\tilde{\sigma} = \sigma \mid \tilde{m} = m, \tilde{\sigma} \neq \perp, \tilde{t} = t] = \Pr_{\mathcal{A}} [\tilde{\sigma} = \sigma \mid \tilde{m} = m, \tilde{\sigma} \neq \perp],$$

$$\Pr_{\mathcal{A}} [\tilde{m} = m \mid \tilde{\sigma} \neq \perp, \tilde{t} = t] = \Pr_{\mathcal{A}} [\tilde{m} = m],$$

- если $\Pr_{\mathcal{A}} [\tilde{\sigma} = \perp, \tilde{t} = t] > 0$, то

$$\Pr_{\mathcal{A}} [\tilde{\sigma} = \sigma \mid \tilde{m} = m, \tilde{\sigma} = \perp, \tilde{t} = t] = \Pr_{\mathcal{A}} [\tilde{\sigma} = \sigma \mid \tilde{m} = m, \tilde{\sigma} = \perp],$$

$$\Pr_{\mathcal{A}} [\tilde{m} = m \mid \tilde{\sigma} = \perp, \tilde{t} = t] = \Pr_{\mathcal{A}} [\tilde{m} = m].$$



Неотслеживаемость по Шеннону

Определение

Схема 2-BS обладает неотслеживаемостью по Шеннону, если

- для любой стенограммы t ,
- для любого распределения $\mathcal{D}_m$, сообщения $m \in M$ и значения подписи $\sigma \neq \perp$,
- для любого нарушителя $\mathcal{A}$,

верно, что:

- если $\Pr_{\mathcal{A}} [\tilde{\sigma} \neq \perp, \tilde{t} = t] > 0$, то

$$\Pr_{\mathcal{A}} [\tilde{\sigma} = \sigma \mid \tilde{m} = m, \tilde{\sigma} \neq \perp, \tilde{t} = t] = \Pr_{\mathcal{A}} [\tilde{\sigma} = \sigma \mid \tilde{m} = m, \tilde{\sigma} \neq \perp],$$

$$\Pr_{\mathcal{A}} [\tilde{m} = m \mid \tilde{\sigma} \neq \perp, \tilde{t} = t] = \Pr_{\mathcal{A}} [\tilde{m} = m],$$

- если $\Pr_{\mathcal{A}} [\tilde{\sigma} = \perp, \tilde{t} = t] > 0$, то

$$\Pr_{\mathcal{A}} [\tilde{\sigma} = \sigma \mid \tilde{m} = m, \tilde{\sigma} = \perp, \tilde{t} = t] = \Pr_{\mathcal{A}} [\tilde{\sigma} = \sigma \mid \tilde{m} = m, \tilde{\sigma} = \perp],$$

$$\Pr_{\mathcal{A}} [\tilde{m} = m \mid \tilde{\sigma} = \perp, \tilde{t} = t] = \Pr_{\mathcal{A}} [\tilde{m} = m].$$



Неотслеживаемость по Шеннону

Определение

Схема 2-BS обладает неотслеживаемостью по Шеннону, если

- ▀ для любой стенограммы t ,
- ▀ для любого распределения $\mathcal{D}_m$, сообщения $m \in M$ и значения подписи $\sigma \neq \perp$,
- ▀ для любого нарушителя $\mathcal{A}$,

верно, что:

- если $\Pr_{\mathcal{A}} [\tilde{\sigma} \neq \perp, \tilde{t} = t] > 0$, то

$$\Pr_{\mathcal{A}} [\tilde{\sigma} = \sigma \mid \tilde{m} = m, \tilde{\sigma} \neq \perp, \tilde{t} = t] = \Pr_{\mathcal{A}} [\tilde{\sigma} = \sigma \mid \tilde{m} = m, \tilde{\sigma} \neq \perp],$$

$$\Pr_{\mathcal{A}} [\tilde{m} = m \mid \tilde{\sigma} \neq \perp, \tilde{t} = t] = \Pr_{\mathcal{A}} [\tilde{m} = m],$$

- если $\Pr_{\mathcal{A}} [\tilde{\sigma} = \perp, \tilde{t} = t] > 0$, то

$$\Pr_{\mathcal{A}} [\tilde{m} = m \mid \tilde{\sigma} = \perp, \tilde{t} = t] = \Pr_{\mathcal{A}} [\tilde{m} = m].$$



Априорная информация

- ▀ $\Pr_{\mathcal{A}} [\tilde{m} = m]$: не зависит от $\mathcal{A}$.
- ▀ $\Pr_{\mathcal{A}} [\tilde{\sigma} = \sigma \mid \tilde{m} = m, \tilde{\sigma} \neq \perp]$: не зависит от $\mathcal{A}$, если схема 2-BS обладает неотслеживаемостью по Шеннону.

Неотслеживаемость по Шеннону

Неотслеживаемость по Шеннону



Совершенная стойкость



Применимо для исследования не всех схем.

- Например, на практике случайные значения вырабатываются с помощью (вычислительно стойких) ГПСП.

Неотслеживаемость по Шеннону vs модель BL

Неотслеживаемость по Шеннону



Применимо для исследования
совершенной стойкости

Модель BL



Применимо для исследования
*совершенной, статистической,
вычислительной* стойкости

Неотслеживаемость по Шеннону vs модель BL

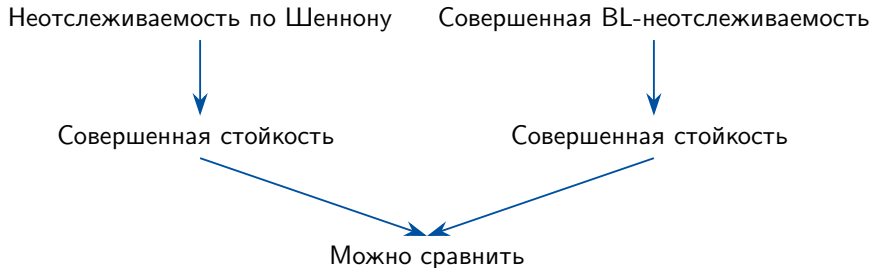
Неотслеживаемость по Шеннону $\longleftrightarrow$? Стойкость в модели BL

Совершенная BL-неотслеживаемость

Определение

Схема 2-BS обладает свойством совершенной BL-неотслеживаемости, если для любого нарушителя $\mathcal{A}$ $\text{Adv}_{2\text{-BS}}^{\text{BL}}(\mathcal{A}) = 0$.

Неотслеживаемость по Шеннону vs совершенная BL-неотслеживаемость



Эквивалентность определений

Теорема

Схема 2-BS обладает совершенной BL-неотслеживаемостью тогда и только тогда, когда она обладает неотслеживаемостью по Шеннону.

Неотслеживаемость по Шеннону $\iff$ Совершенная BL-неотслеживаемость

Эскиз доказательства

Идея: так как оба определения формулируются в терминах теоретико-информационной стойкости, можно сделать переход к детерминированным нарушителям.

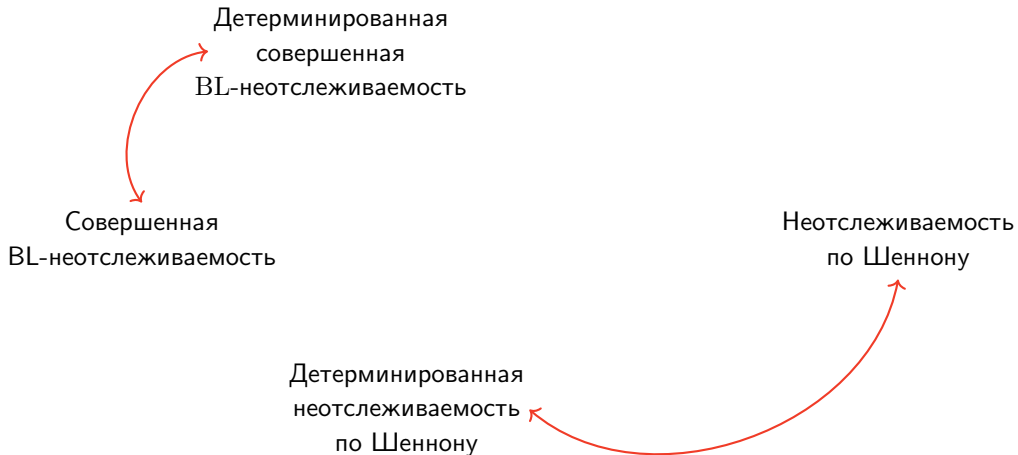
Эскиз доказательства

Совершенная
BL-неотслеживаемость

Неотслеживаемость
по Шеннону



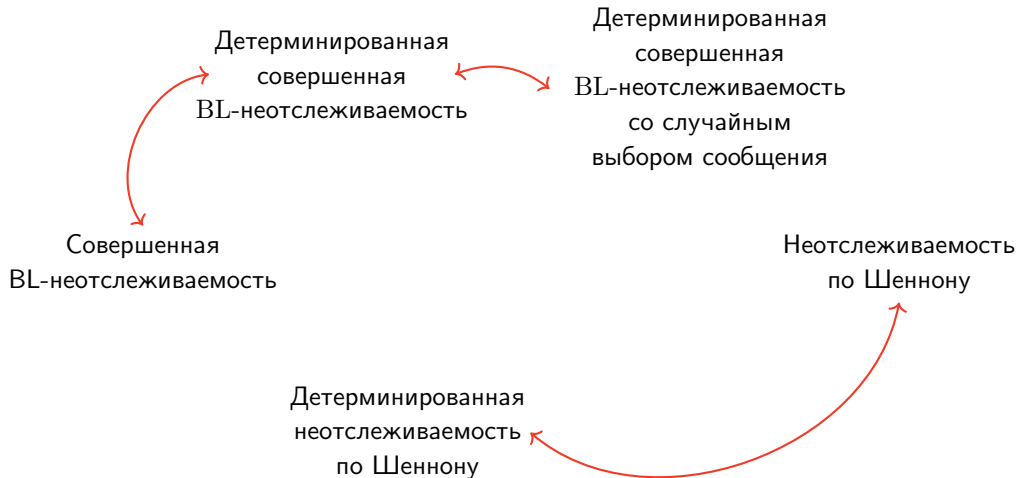
Эскиз доказательства



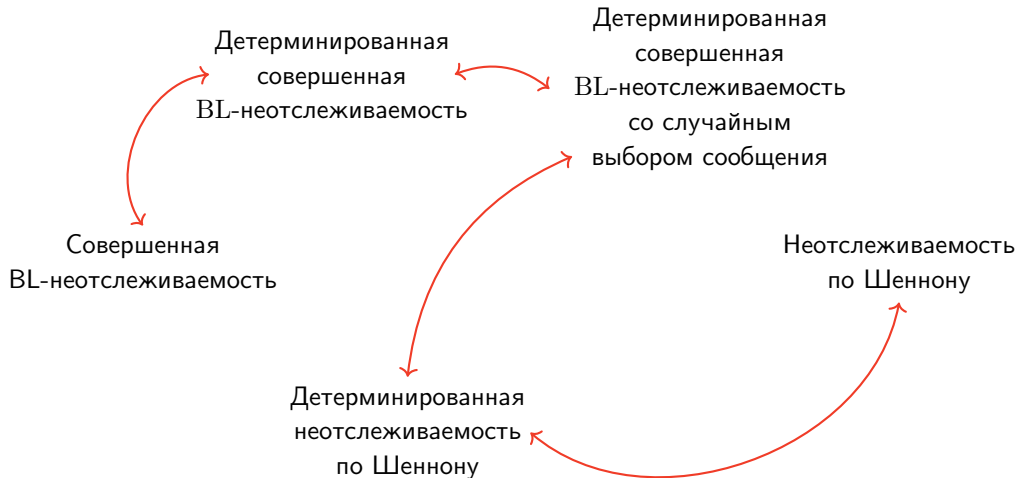
Эскиз доказательства

Идея: в модели BL сообщения выбираются нарушителем, в неотслеживаемости по Шеннону в соответствии с распределением → определим промежуточное свойство.

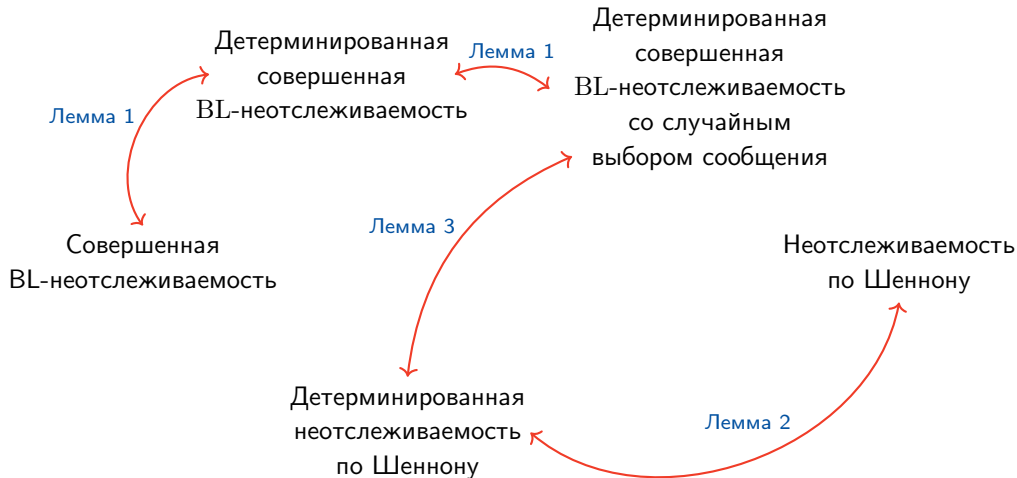
Эскиз доказательства



Эскиз доказательства



Эскиз доказательства

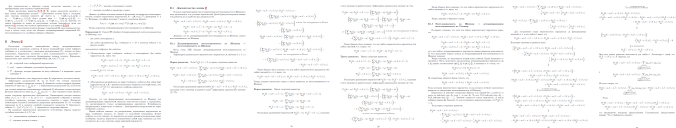


Доказательство

Лемма 1.



Лемма 2.



Лемма 3.



...



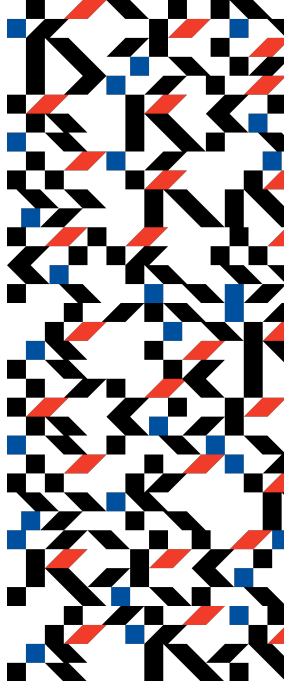
Спасибо за внимание!

Утехина Мария Павловна, utekhina@cryptopro.ru

Ахметзянова Лилия Руслановна

Смышляев Станислав Витальевич

01.06.2026



Модель BL

Определение

Для схемы 2-BS преимущество нарушителя $\mathcal{A}$ задается как

$$\text{Adv}_{2\text{-BS}}^{\text{BL}}(\mathcal{A}) = \left| \Pr[\mathbf{Exp}_{2\text{-BS}}^{\text{BL}}(\mathcal{A}) \rightarrow 1] - \frac{1}{2} \right|,$$

где эксперимент $\mathbf{Exp}_{2\text{-BS}}^{\text{BL}}(\mathcal{A})$ определён на рисунке далее.



Модель BL

$\text{Exp}_{2\text{-BS}}^{\text{BL}}(\mathcal{A})$

$b \xleftarrow{\mathcal{U}} \{0, 1\}$

$b_0 \leftarrow b$

$b_1 \leftarrow 1 - b$

$st \leftarrow \mathcal{A}^{\text{Init}}()$

$b' \leftarrow \mathcal{A}^{\text{User}_1, \text{User}_2}(st)$

return $(b' = b)$

Oracle $\text{Init}(\text{pk}, m_0, m_1)$

$\text{sess}_0 \leftarrow \text{init}$

$\text{sess}_1 \leftarrow \text{init}$

store (pk, m_0, m_1)

return θ

Oracle $\text{User}_1(i, t_i^1)$

if $i \notin \{0, 1\} \vee \text{sess}_i \neq \text{init}$: **return** $\perp$
 $\text{sess}_i \leftarrow \text{open}$

$(t_i^2, \text{state}_i) \leftarrow 2\text{-BS.User}_1((\text{pk}, m_{b_i}), t_i^1; r)$

return t_i^2

Oracle $\text{User}_2(i, t_i^3)$

if $\text{sess}_i \neq \text{open}$: **return** $\perp$

$\text{sess}_i \leftarrow \text{closed}$

$\sigma_{b_i} \leftarrow 2\text{-BS.User}_2(\text{state}_i, t_i^3; r)$

if $\text{sess}_0 = \text{sess}_1 = \text{closed}$:

if $\sigma_{b_0} \neq \perp \wedge \sigma_{b_1} \neq \perp$: $\text{out}_0 = \sigma_0, \text{out}_1 = \sigma_1$

if $\sigma_{b_0} = \perp \wedge \sigma_{b_1} = \perp$: $\text{out}_0 = \perp, \text{out}_1 = \perp$

if $\sigma_{b_0} = \perp \vee \sigma_{b_1} \neq \perp$: $\text{out}_0 = \perp, \text{out}_1 = \theta$

if $\sigma_{b_0} \neq \perp \vee \sigma_{b_1} = \perp$: $\text{out}_0 = \theta, \text{out}_1 = \perp$

return $(\text{out}_0, \text{out}_1)$

return θ

